ASP | AI IMPERATIVE 2030

COLUMBIA | SIPA

Photo Credit: U.S. Department of Energy

SPUTNIK REPORT

Securing the Stack:

Futureproofing U.S. AI Infrastructure Defense

www.AmericanSecurityProject.org

June 2026

Securing the Stack:
Futureproofing U.S. AI Infrastructure Defense

Artificial intelligence systems that execute tasks without human oversight or produce the primary basis for federal decision-making are being rapidly embedded across U.S. government, defense, and infrastructure systems. Continuity of compute is now a national security priority, as interruptions within the data centers that run these sophisticated algorithms can put vital national functions at risk. Addressing the growing disparity between the strategic importance of AI and the security and resilience of its underlying infrastructure is vital to prevent data center disruptions from triggering cascading failures across other critical systems.

Power disruptions, kinetic threats, and cyberattacks pose the most acute threats to AI data centers and the national functions they support. An additional investment over current projections of at least $500 billion in AI compute generation[1] and $2 billion in cyber and physical defenses[2] by 2030 is necessary to close existing gaps. For these investments to succeed, however, Washington needs to expedite power permitting reform, establish federal physical and cybersecurity baselines for data centers, and create a cross-sector coordination authority to address water, power, and data infrastructure dependencies.

The Problem

- **Grid instability and kinetic, physical, and cyber attacks on AI data centers can cause cascading disruptions across other connected critical infrastructure systems.**
- **Data center redundancy and compute availability are necessary to maintain continuity of compute in the case of disruption, but demand for AI compute currently outpaces available supply.**
- **A disjointed and overlapping web of regulations slows infrastructure expansion and drives market concentration, creating single points of failure at the national scale.**

The Solution

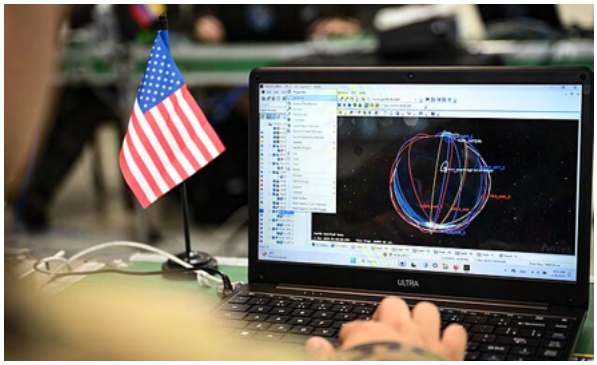
- **Designate AI data centers as the 17th critical infrastructure sector under CISA, establish federal cybersecurity and physical security baselines, and increase funding and personnel at CISA.**
- **Additional data centers are needed to increase redundancy and compute availability, which requires acceleration of energy generation and permitting reform.**
- **Establish a cross-sector interagency coordination mechanism to address dependencies, improve federal coordination, and streamline threat-assessment and emergency response management.**

This project was conducted alongside graduate researchers at the Columbia University School of International and Public Affairs between February 2026 and June 2026. The authors thank the research team for their contributions to this report.

Introduction

On the first day of his second term, President Donald J. Trump announced an ambitious national strategy to strengthen American global leadership by accelerating the adoption of artificial intelligence and multiplying the processing power, or "compute," available to support it. Released in July 2025, *Winning the Race: America's AI Action Plan* pursued these goals through two notable federal actions: first, it declared data center construction a national security imperative, and second, it directed federal agencies and critical infrastructure (CI) providers to integrate artificial intelligence (AI) into their day-to-day operations.

As we approach the one-year anniversary of the *AI Action Plan*, it is vital to acknowledge the enormous progress made in increasing compute supply and demand in the United States. On the supply side, more than $500 billion has flowed into new AI data centers in one of the largest coordinated capital investment cycles in history. On the demand side, upwards of 90% of federal workers are using or planning to use AI,[3] joining the 60% of U.S. CI operators who have already adopted the technology.[4] These accomplishments have protected U.S. infrastructure from cyberattacks, made public and private workflows more efficient, and saved taxpayers billions of dollars[5] while cementing America's reputation as a global leader in AI adoption.



A National Guard systems operator works through a critical infrastructure cyber scenario. Department of War photo.

As artificial intelligence technologies improve in both capability and reliability, they are rapidly becoming embedded across America's most sensitive national functions. More than 440 documented AI adoptions in the public sector are "high-impact,"[6] meaning their outputs serve as the primary basis for decisions with significant effects on U.S. citizens or national security.[7] Over half of agencies are adopting agentic AI systems,[8] which make decisions and take actions independent of human operators. In addition to autonomously handling government functions like managing logistics, identifying cyber intrusions, and assisting law enforcement, AI agents are managing complex tasks in nearly every critical infrastructure sector, including emergency response management,[9] transportation,[10] telecommunications, banking, and healthcare.

As agentic and high-impact AI systems are increasingly interconnected with and responsible for managing critical and complex workflows, disruptions of these systems can jeopardize the continuity of vital national functions. As a result, the data centers that run these systems are valuable strategic assets — and increasingly lucrative targets for espionage, cyberattacks, sabotage, and kinetic warfare. "Continuity of compute," or ensuring AI data centers remain operational in the case of disruption from either intentional threats or unintentional failures, is now of critical national importance.

Despite this, the data center industry lacks a CI designation under the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), the governing framework that triggers federal coordination, security standards, and resilience requirements for the nation's most vital systems. As a result, no federal agency is responsible for analyzing novel risks, coordinating with industry, and leading a national response when data center infrastructure is targeted. While many safety-critical AI systems are held to heightened security standards under a web of state and sector-specific regulations, a streamlined federal framework is urgently needed to reduce barriers to infrastructure expansion and update data center security for the AI era. This report identifies the most acute vulnerabilities that Congress must address either within such a framework or separately in the near term.

Physical Threats to U.S. AI Infrastructure

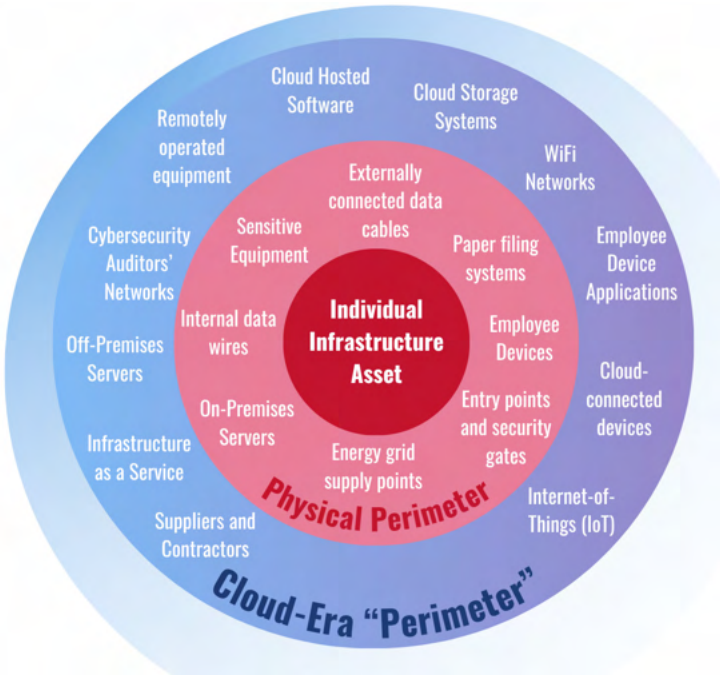
As federal agencies and infrastructure operators begin to rely on artificial intelligence tools for day-to-day decision-making, cybersecurity, and emergency management, the data centers that host them have become increasingly valuable targets for physical attacks. A physical attack is when an individual or group leverages physical access to people, property, and equipment to cause theft, espionage, or localized damage. Up from just 40% in 2024, 61% of surveyed professionals now cite physical security as a leading threat to U.S. data centers – above ransomware and other cyber threats.[11]

Insider Threats

Insiders can abuse their authorized access to a CI system to conduct harms such as espionage, sabotage, or cyberattack prepositioning. A malicious actor with physical access to an AI data center may damage network equipment, steal intellectual property, sabotage software or hardware, or permanently destroy AI servers.[12] Saboteurs can also halt data center operations by gaining access to upstream water and energy infrastructure. Attacks on these systems can cause AI system failures that can interrupt operations across connected infrastructure, including downstream data centers running additional infrastructure systems. Such a cascade of failures would pose a substantive risk to U.S. national security.

As data centers aren't federally classified as a standalone CI sector, there is no federal requirement mandating security clearance or background checks for personnel with access to AI data centers.[13] Federal AI systems hosted on the commercial cloud must follow FedRAMP physical security requirements designed to deter inside threats. However, between 70-77% of CI operators are privately owned and therefore not subject to FedRAMP.[14] These operators are governed by a complex patchwork of sector-specific regulations, voluntary guidelines, and state laws, few of which establish physical security baselines for connected data center infrastructure.[15]

U.S. Infrastructure Points of Attack



Supply Chain Threats

Physical components can also grant U.S. competitors or adversaries access to sensitive data, software, or hardware within data centers. Power distribution units, cooling controllers, building management systems, and fire suppression controls are sourced from a small set of vendors with opaque supply chains. American tech companies regularly source high-value manufactured components from China, including printed circuit boards (Victory Giant Tech), optical transceivers (Innolight), and more recently, liquid cooling technology (Lingyi iTech and Feilong Auto Components).[16] In addition to the threat posed by covertly implanted surveillance or disruptive technology within these components, overreliance on sophisticated hardware from adversarial suppliers pose significant threats to the internal integrity of American AI data centers and their interconnected infrastructure systems.

State and Non-State Actor Threats

While industry surveys indicate that insider breaches are five times more frequent than those from external actors,[17] physical intrusions from state and non-state actors can impose highly destructive costs to AI data centers and the infrastructure they support. Protesters and anti-AI groups have launched homemade explosives at external-facing data center components like power generators and energy support systems, with intelligence agencies warning of the potential for escalating future attacks.[18]

While physical attacks on domestic data centers are more likely to be conducted by U.S. persons than state-sponsored actors, espionage and sabotage are common state-sponsored activities. Security firms have exposed a range of actors who have gained unauthorized physical access to data centers, with the likeliest and most capable perpetrators being rival countries.[19] However, a lack of mandatory reporting requirements means that these intrusions are rarely reported to related agencies or the public, making it difficult to understand the scale and potential impact of these activities.

Environmental Threats

Environmental hazards also pose a physical risk to U.S. data centers. Of the 97 data center markets tracked by analytics firm First Street, 79% are exposed to acute climate exposure risk from flooding, extreme wind, wildfire, and other hazards.[20] Extreme weather events can damage AI data centers and their surrounding infrastructure, taking systems offline either temporarily or permanently. In the long run, gradually worsening climate trends are predicted to impact data center operations by imposing higher housing and insurance costs, tighter regional capacity, and weaker uptime during extreme weather.[21]

Hurricane Helene destroys a railroad bridge in North Carolina. U.S. Department of Commerce photo.

Cyber Threats to American AI Infrastructure

Cyberattacks pose significant danger to the security and resilience of AI data centers. While these attacks have historically been enacted for espionage or surveillance purposes, cyber intrusions with the capability for destruction are of increasing concern. In 2024, hackers associated with the Security Service of Ukraine claimed to have virtually destroyed a data center used by Russian military, energy, and telecommunications operators.[22] These trends are expected to worsen as artificial intelligence proliferates and becomes vital to the operations of the federal government.[23]

State-Sponsored Pre-Positioning Against Critical Infrastructure

State-affiliated cyber operations have shifted from intelligence collection to "capability pre-positioning," or the establishment of persistent access to critical networks through an initial cyber intrusion. Remotely activated "cyber bombs" planted within water, energy, and telecommunications systems can each provide pathways for adversaries to disrupt data center operations.

Advanced Persistent Threat (APT) groups linked to the Chinese government have increasingly targeted U.S. CI for capability pre-positioning. Volt Typhoon is disruption-focused and targets OT systems in energy, water, transportation, communications, and government installations. In February 2024, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported with high confidence that China had maintained persistent access to U.S. communications, energy, transportation, and water sector networks for at least five years, with the explicit aim of disrupting critical functions in the event of a conflict over Taiwan.[24] The FBI identified approximately 200 U.S. CI entities compromised in the campaign, including the New York Metropolitan Transportation Authority, thirteen gas pipeline operators, major telecommunications service providers, Houston's port, and other critical public infrastructure.[25] Exemplifying the breadth and duration of the group's operational successes, Volt Typhoon operated for ten months inside the Littleton Electric Light and Water Department in Massachusetts, a small-town municipal utility that controls both electric distribution and the treatment of drinking water.[26]

Water Infrastructure Dependencies

A medium-sized data center cooling system consumes approximately 110 million gallons of water annually, with larger facilities drawing up to 5 million gallons per day.[27] The Houston Advanced Research Center projects data center water use will reach 49 billion gallons in Texas alone in 2025 and up to 399 billion gallons by 2030, equivalent to 6.6 percent of total state water use.[28] Cooling system failure can produce cascading shutdowns, equipment damage, and even hardware destruction.[29]

In November 2023, Iran's Islamic Revolutionary Guard Corps, operating as CyberAv3ngers, exploited Unitronics Vision Series programmable logic controllers at the Municipal Water Authority of Aliquippa, Pennsylvania, defaced the operator interface, and forced the system into manual operation.[30] Controller families of the type exploited at Aliquippa are widely deployed across water and wastewater environments, including the kinds of municipal systems on which major data center corridors depend. Iran-linked targeting of programmable logic controllers continued until April 2026, when the North American Electric Reliability Corporation (NERC) confirmed it was monitoring the bulk power system for renewed Iran-linked PLC threats.[31]

Most water systems serving major data center clusters are municipal utilities or rural cooperatives operating with minimal IT staff, outdated supervisory control and data acquisition (SCADA) systems, and single-vendor cloud platforms.[32] Despite these risks, little research exists on the security vulnerabilities of the water systems that AI data centers depend upon.[33] While CISA assigns sector-specific protocols to water and information technology, no federal entity bridges the intersection between them.

Industrial Control Systems

In addition to consistent access to water and power, AI data centers depend on industrial control systems that can be targeted by U.S. rivals and adversaries. These include cooling systems, fire-suppression mechanisms, access control systems, water pump stations, power distribution units, and power supply systems. CISA red team assessments have repeatedly identified exploitable weaknesses in OT environments; despite this, industrial SCADA software suites with known vulnerabilities remain widely deployed.[34] NERC's January 2026 CIP Standards Roadmap rated the insider threat to the bulk power system at a likelihood of 3.75 and an impact score of 4.67, the highest in its assessment.[35] AI data centers operating in the same regions carry no equivalent rating because they lack federal CI standards.

Energy Infrastructure Dependencies

AI data centers function as both supply chain risks and instruments for attack against the energy grids that power them. Coordinated cyber actors can leverage workload scheduling and switching to induce sudden power surges or drops of more than 100 megawatts at a single facility, with the potential to trigger cascading failures across connected distribution networks.[36] In September 2025, NERC documented inadequate modeling and operating protocols for integrating large data centers into the bulk power system. Months later, data centers began unexpectedly disconnecting from the Eastern and Texas Interconnections, leading to changes to modeling, monitoring, and commissioning practices for large data center loads.[37] Additional research is needed to ensure that data centers can continue critical government computing processes in the event of an attack or disruption.

Federal Cybersecurity Regulations and Policy Gaps

In 2011, U.S. agencies began moving federal information systems from outdated localized servers to commercial cloud networks under standardized security baselines governed by FedRAMP.[38] In 2023, the Federal Data Center Enhancement Act expanded mandatory cybersecurity and operational requirements to enhance the baseline physical security and resiliency of federal agency data centers.[39] Section 1543 of the FY2026 National Defense Authorization Act requires the Department of Defense to conduct a study by December 2026 on how to deter adversaries from conducting cyberattacks on U.S. defense data systems and the infrastructure that supports them.[40]

Despite these efforts, a distinct gap in regulatory authority over AI datacenters exists within NSM-22, issued April 30, 2024, which designates 16 CI sectors and assigns each a Sector Risk Management Agency (SRMA) with authority to set minimum security requirements.[41] Because AI datacenters do not have their own CI designation, they fall under various CI sectors and face differing SRMAs, preventing a coherent and harmonized regulatory ecosystem. The Cybersecurity Information Sharing Act of 2015, which provided liability protections that empowered private operators to share cyber threat indicators with the federal government, lapsed in September 2025, compounding the issue of consistent reporting. Although it was temporarily extended through September 30, 2026, this act will soon lapse again.[42] Furthermore, existing inspection and compliance regimes regarding data centers focus on site-specific security and resilience, but critical upstream operational technology (OT) systems are under the jurisdiction of separate regulatory bodies. This lack of regulatory harmonization creates security gaps which can be exploited by adversaries.

Kinetic Threats to American AI Infrastructure

The AI Action Plan aims to promote global adoption of cutting-edge technologies by exporting American AI software and hardware through bilateral engagements with partner countries.[43] While most foreign imports of U.S. technologies and infrastructure occur in secure territories, the increased kinetic targeting of data centers in conflict zones raises important questions about the rising geostrategic importance of what was once considered purely civilian infrastructure.

Attacks on U.S. Data Centers Abroad

On March 1, 2026, Iran's Islamic Revolutionary Guard Corps struck three AWS facilities in the United Arab Emirates and Bahrain using drones, in the first publicly confirmed military attack on AI-capable data centers.[44] Iranian state media was explicit about the rationale: the data centers were targeted to investigate whether the U.S. hosted military and intelligence activities on these data centers.[45]

This is the threat environment in which American-built data centers abroad now operate. The United States has active or planned Stargate deployments in Norway, Japan, and additional partner nations under the "OpenAI for Countries" initiative.[46] Each of these regions present distinct operational risks to AI infrastructure, spanning from territorial disputes in the Indo-Pacific to the proximity of Russian pressure in Northern Europe.

Aftermath of an Israeli bombing on IRGC facilities in Tehran on June 15, 2025. Photo by Avash Media under creative commons 4.0.

Implications for AI Diplomacy and Alliance Credibility

If American-linked AI infrastructure increasingly becomes a target during conflicts, states may turn to Chinese firms instead of American companies due to the associated geopolitical risks. Through Beijing's Digital Silk Road project, countries throughout the Middle East are already deploying digital infrastructure projects owned and operated by Huawei, ZTE, and Alibaba.[47]

Improved security and resilience could be a selling point for U.S. infrastructure abroad. The AI Action Plan calls for high-security data center standards for military and intelligence use; however, those standards have yet to be produced.[48] At the same time, no legal framework currently defines the U.S. government's security obligations toward privately owned, U.S.-linked AI infrastructure operating abroad, nor does any framework establish liability if those systems are disrupted during crisis or conflict. This ambiguity raises broader strategic questions regarding the extent of U.S. commitments to AI infrastructure developed in coordination with partner nations and the long-term reliability of American-linked digital ecosystems operating in contested geopolitical environments.

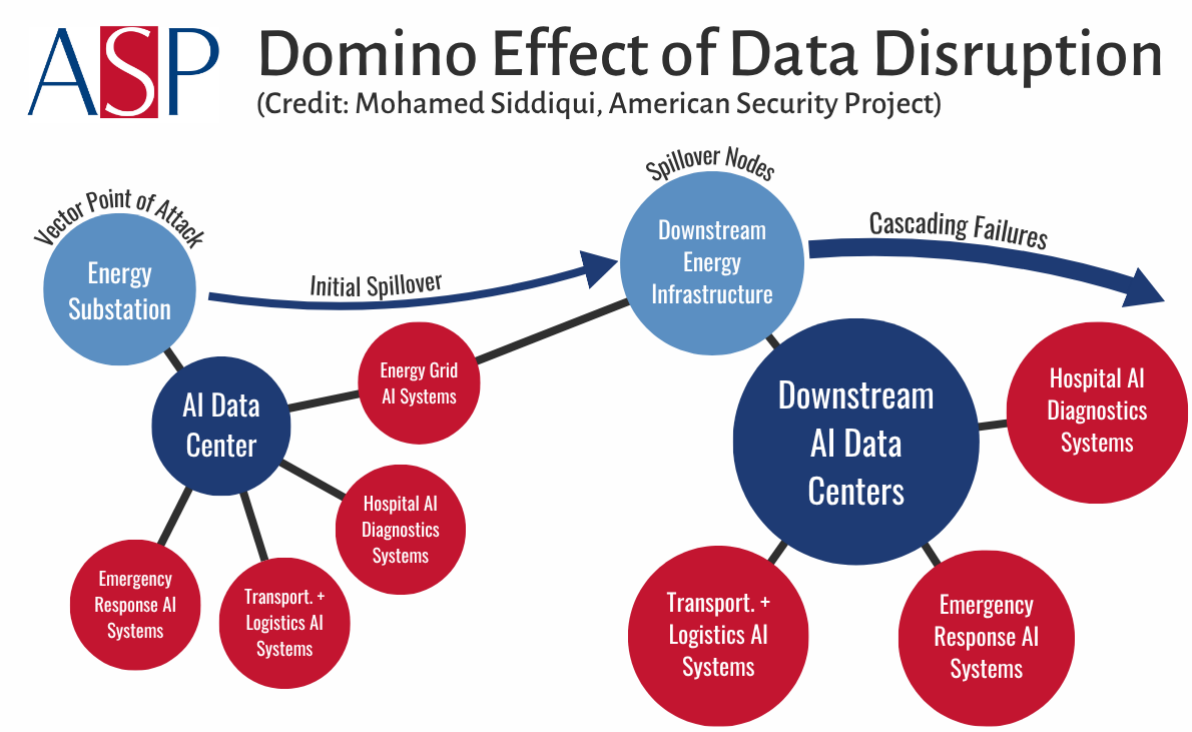
Powering a Resilient and Redundant System

Limited power supply is currently the most significant constraint to data center construction, slowing down the development of "hyperscale" and "edge" facilities that serve as the "brain" and "nerves" of artificial intelligence. An estimated 60% of planned data center capacity for 2027 is at a standstill as of May 2026,[49] slowing U.S. data center expansion and potentially threatening grid resilience and reliability.

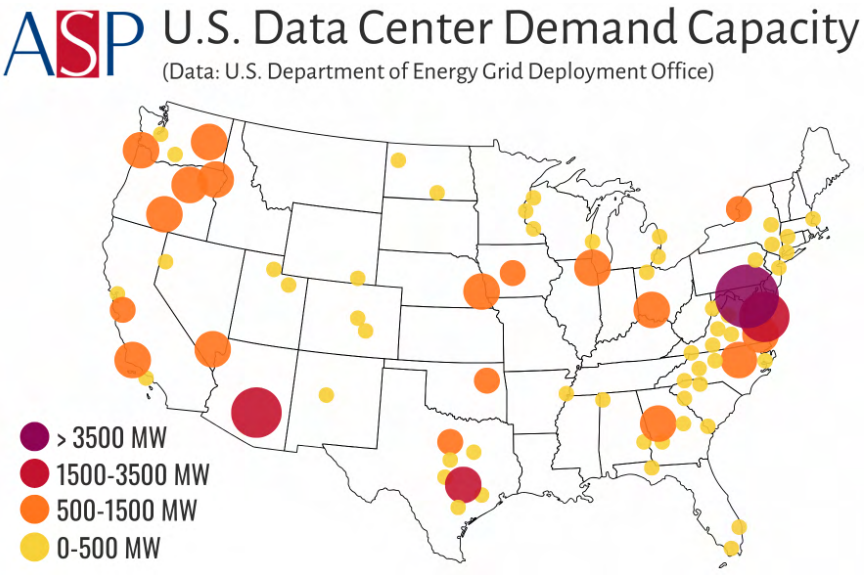
The Security Imperative for AI Data Center Expansion

A sufficient cushion of available compute is required to avoid the most catastrophic effects caused by data center interruptions. A fully "fault-tolerant" data center architecture requires 2N or 2N+1 redundancy; this means the entire system is duplicated, including power, cooling, and AI hardware.[50] For the most extreme threats, zonal redundant systems and geographic redundant systems are central to building a resilient network of data centers on stand-by.[51] Within this ecosystem, high-impact data and operations systems are dispersed across different data centers within the same region or hundreds of miles away to survive external and internal regional events. To reach full reliability, more data centers are needed as well as additional electricity for power and cooling at each location.

Without intervention, the imbalance between electrical supply and demand can cause a "domino effect" with negative consequences for the entire electrical grid. Brookings estimates that seven of thirteen major U.S. grid regions are projected to operate below their critical safety margins by 2030, significantly increasing the risk of blackouts.[52] Potential consequences include more frequent power outages, the implementation of rolling blackouts to manage load, and extreme price volatility during peak periods. Given the increasing interconnectedness of American public and private infrastructure, the potential effects compound as multiple systems experience electricity shortages or damage from an isolated malicious act.



State Level Regulatory Approaches and Constraints



Despite the need for federal intervention, key parts of the data center power bottleneck remain outside federal control. Distribution networks remain under state jurisdiction, regulated by public utility commissions that control project rate-setting, approvals, and timelines. Federal laws cannot override state commission proceedings, impose binding timelines on state-level decisions, or substitute for local land use and zoning approvals.[53] Congress has also not yet produced a comprehensive framework for cost allocation, cross-jurisdictional coordination, or standardized timelines across the federal, state, and local approval process. As a result, energy-oriented data center legislation primarily exists on the state level and varies from state to state.[54]

Texas is the only major data center cluster where aggregate energy supply is forecasted to be sufficient to meet demand through 2030.[55] This is due to the Electric Reliability Council of Texas's (ERCOT) deregulated structure, which operates without a federal interconnection queue and provides clear cost allocation rules for grid upgrades. The second-largest data center capital investment cluster spans both Pennsylvania and Virginia, representing approximately $125 billion in new AI data center investment.[56] Pennsylvania and Virginia are serviced by PJM Interconnection, which in December 2025 failed for the first time to secure enough committed power supply for 2027 and 2028. The shortfall was about 6.6 GW below the reserve capacity needed to maintain reliability, with data centers accounting for about 97% of projected demand growth.[57] In Virginia, Dominion Energy currently supplies approximately 4 GW of data center load but has committed to roughly 51 GW of future demand.[58] The pipeline of new energy supply is limited, with approximately 9 GW of projects expected to reach commercial operation by 2030. Energy infrastructure projects remain constrained by PJM's interconnection queue, even as the reformed cycle-based process now targets a one- to two-year review timeline. Improving interconnection efficiency is therefore critical to grid stability in the PJM region.

Federal Responses and Challenges

For federal agency use-cases, FedRAMP requires high impact Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service providers to maintain adequate data center redundancy based on specific recovery goals and a tailored risk assessment.[59] Even though overall data center availability remains at 1 percent and will likely continue to be in coming years, this ensure that critical federal systems will maintain the redundancies necessary to maintain resilience in the case of disruption.[60] However, these federal regulations are not extended to commercial AI data centers, putting private and state-managed U.S. CI operations at risk.

The Federal Energy Regulatory Commission (FERC) governs access to the interstate transmission system. While FERC's Order 2023 moved to batched, cluster-based processing[61] and Order 1920 pushes transmission providers toward longer-term regional planning to anticipate large load growth,[62] these reforms require local grid operators to align compliance processes, accelerate regulatory approval, and work through existing backlogs according to new standards. As a result, they are unlikely to shorten queue timelines over the next 1–3 years.[63]

Policy Recommendations

As U.S. federal agencies and infrastructure operators increasingly trust AI systems to manage vital workflows, securing their underlying infrastructure is vital to sustaining critical national functions in a crisis. Urgent federal action is needed for policymakers and infrastructure operators to catch up to the AI era and protect U.S. critical infrastructure from disruption.

To Ensure America's Critical Infrastructure is Defended Against AI-Powered Threats:

Designate AI Data Centers as the Seventeenth Critical Infrastructure Sector under CISA. NSM-22 tasks CISA with protecting 16 listed CI sectors from cyber threats, climate disasters, and kinetic attacks from foreign adversaries. The framework establishes sector-specific risk management, cross-sector coordination, and a statutory pathway for incident reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Without CI designation, CIRCIA minimum reporting standards cannot be uniquely applied to the data center industry, and no agency carries lead-coordinator responsibility when novel physical or cyberattacks occur.[64]

To treat AI data centers as critical infrastructure, President Trump should amend NSM-22 to add AI data centers as the seventeenth CI sector or replace the memorandum with a new version. Alternatively, Congress could pass H.R. 5927, the Securing Reliable Power for Advanced Technologies Act, which would extend Defense Production Act authority to designated AI infrastructure projects. H.R. 5927 uses a different threshold for covered critical AI infrastructure; this report recommends the EO 14318 threshold for sector designation to focus federal oversight on the largest and most strategic facilities.[65]

Cover AI data centers under CIRCIA and reauthorize CISA 2015. The data center industry lacks critical threat mitigation standards, preventing a coordinated federal response. CISA, in coordination with NIST, should publish minimum cybersecurity standards for AI data centers calibrated to workload sensitivity, facility scale, and the criticality of shared grid and water dependencies. The Department of Homeland Security (DHS) should apply forthcoming CIRCIA facility-level reporting requirements to designated facilities, and Congress should establish a permanent policy to function in place of Cybersecurity and Information Sharing Act of 2015's temporary renewal which expires on September 31st, 2026.

Establish a cross-sector interagency coordination authority to address water, grid, and data center dependencies. Network segmentation and defense-in-depth approaches prevent penetrations of a cloud environment from spreadingFederal CI regulations treat water, energy, communications, and information technology as separate sectors with little interagency communication. Establish, by interagency agreement under CISA leadership, a permanent coordination mechanism among the SRMAs for water (Environmental Protection Agency), energy (Department of Energy), communications (DHS/CISA), and the new AI data center sector (DHS/CISA), with mandatory dependency mapping, joint red-team exercises modeled on CISA's November 2024 CI assessment. FERC's RM26-4-000 large-load interconnection proceeding addresses cost allocation and reliability for large-load interconnection, but a cross-sector mechanism is necessary to close the cybersecurity oversight gap.

About the Authors

Courtney Manning is the Director of *AI Imperative 2030* at the American Security Project, where she leads a team of cross-disciplinary stakeholders investigating the critical geostrategic forces driving the global AI race in the 21st century.

Tyler Matos is a senior pursuing a Bachelor's in International Affairs at the George Washington University who specializes in International Politics, Great Power Competition, and Energy Security.

Elle Baker is an International Security and Diplomacy student pursuing a Master of International Affairs at the Columbia University School of International and Public Affairs (SIPA) who specializes in Climate Security, Conflict Resolution, and Public Diplomacy.

Tobias Shapiro is a graduate student in the Security Studies Program (SSP) at Georgetown University's Walsh School of Foreign Service, specializing in Russian Military Affairs, International Affairs, and Information Warfare.

Mohamed Siddiqui is an International Security and Diplomacy student pursuing a Master of International Affairs at the Columbia University School of International and Public Affairs (SIPA) specializing in Public Diplomacy, Intergovernmental Organizations, and Strategic Competition.

Endnotes

1 David Crawford et al, "How Can We Meet AI's Insatiable Demand for Compute Power?" *Bain & Company*, September 23, 2025, https://www.bain.com/insights/how-can-we-meet-ais-insatiable-demand-for-compute-power-technology-report-2025/.

2 Encor Advisors, "How Much Does a Data Center Cost? The Complete Guide To 2026 Price Breakdown," June 15, 2026, https://encoradvisors.com/data-center-cost/.

3 Jim Kelly, "New Google Public Sector research shows that nearly 90% of federal agencies are already using AI," *Google Cloud Blog*, January 13, 2026, https://cloud.google.com/blog/topics/public-sector/new-google-public-sector-research-shows-that-nearly-90-of-federal-agencies-are-already-using-ai.

4 Eric Geller, "Safety-critical industries wary about using AI for cybersecurity," *CybersecurityDive*, August 27, 2025, https://www.cybersecuritydive.com/news/artificial-intelligence-cybersecurity-tools-business-adoption-survey-arctic-wolf/758698/.

5 Natalie Alms, "AI tools helped Treasury recover billions in fraud and improper payments," *NextGov*, October 18, 2024, https://www.nextgov.com/artificial-intelligence/2024/10/ai-tools-helped-treasury-recover-billions-fraud-and-improper-payments/400368/.

6 Federal AI Use Case Inventory, U.S. Government Office of Management and Budget, June 2026, https://github.com/ombegov/2025-Federal-Agency-AI-Use-Case-Inventory.

7 Russel Vought, "MEMORANDUM M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government," United States Executive Office of Management and Budget, April 3, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf.

8 Emily Wolfteich, "From Adoption to Accountability," *Government Executive*, May 5, 2026, https://www.govexec.com/insights/whitepaper/adoption-accountability/413301/?oref=ge-insights-lander-river.

9 "AI as Critical Infrastructure: The Next American Lifeline," U.S. Chamber of Commerce Foundation, May 5, 2026, https://www.uschamberfoundation.org/disasters/ai-as-critical-infrastructure-the-next-american-lifeline.

10 "How Freight Railroads Use Technology," Association of American Railroads, accessed May 31, 2026, https://www.aar.org/freight-rail-tech/#!.

11 Bill Kleyman, 2026 State of the Data Center, AFCOM, https://cdn.ymaws.com/afcom.com/resource/resmgr/resource_center/whitepapers/afcom_stateofdatacenter26_ex.pdf.

12 Bennett Tomlinson, "Data Center Security Standards for AI: A Gap Analysis," *Foundation for American Innovation*, February 25, 2026, https://www.thefai.org/posts/data-center-security-standards-for-ai-a-gap-analysis.

13 Cybersecurity and Infrastructure Security Agency, "Resources For Onboarding and Employment Screening," Accessed 18 June, 2026, https://www.cisa.gov/sites/default/files/2024-07/resources-for-onboarding-and-employment-screening-fact-sheet_07-25-2024_508.pdf.

14 Jacob Azrilyant et al., "Fact and Fiction: Demystifying the Myth of the 85%," *George Washington University,* May 6, 2022, https://www.scribd.com/document/575971848/Fact-and-Fiction-85-and-Critical-Infrastructure.

15 https://homeland.house.gov/2026/04/23/media-advisory-subcommittee-chairman-ogles-announces-hearing-on-combating-cyber-threats-to-telecom-networks-data-centers-satellites/; CMS physical security requirements govern health care companies that manage HIPAA data, https://security.cms.gov/policy-guidance/physical-environmental-protection-pe

16 Reuters, "Google in Talks With China's Envicool, Others to Buy Data Centre Cooling Systems, Sources Say," March 17, 2026, https://www.reuters.com/world/china/google-talks-with-chinas-envicool-others-buy-data-centre-cooling-systems-sources-2026-03-17/.

17 IBM Cost of a Data Center Breach Report 2025, IBM, https://www.ibm.com/reports/data-breach.

18 Daniel Boguslaw, US Law Enforcement Warns of 'Anti-Tech Extremism' as AI Hatred Grows, *Wired*, May 26, 2026, https://www.wired.com/story/us-law-enforcement-warns-of-anti-tech-extremism/.

19 Ben Sherry, "Guards, Guns, and the Billion-Dollar Race to Protect the Hottest New Target for Criminals—Data Centers," *Inc.*, June 10, 2026, https://www.inc.com/ben-sherry/want-to-get-rich-in-the-ai-boom-guard-data-centers/91327059.

20 "79% of Global Data Center Capacity Faces Elevated Climate Risk," *PR Newswire,* June 18, 2026, https://www.prnewswire.com/news-releases/79-of-global-data-center-capacity-faces-elevated-climate-risk-302804645.html.

21 Georgia Fearn, "The Hidden Threat to the AI Boom No One Is Talking About," *Inc.*, June 18, 2026, https://www.inc.com/georgia-fearn/the-hidden-threat-to-the-ai-boom-no-one-is-talking-about/91362740.

22 Martin Fornusek, "Sources: Ukrainian hackers destroy data center used by Russian military industry," *Kyiv Independent,* April 8, 2024, https://kyivindependent.com/sources-ukrainian-hackers-destroy-data-center-used-by-russian-military-industry/.

23 CrowdStrike, "2024 CrowdStrike Global Threat Report," February 21, 2024, https://ir.crowdstrike.com/news-releases/news-release-details/2024-crowdstrike-global-threat-report-breakout-breach-under/; CrowdStrike, "2025 Threat Hunting Report," August 19, 2025, https://go.crowdstrike.com/2025-threat-hunting-report.html.

24 Congress.gov, "Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications," June 18, 2026, https://www.congress.gov/crs-product/IF12798; U.S. House Committee on Homeland Security, letter from Chairman Mark Green, Subcommittee Chairman Andrew Garbarino, and Subcommittee Chairman Josh Brecheen to DHS Secretary Kristi Noem, March 17, 2025, https://homeland.house.gov/wp-content/uploads/2025/03/2025-03-17-Green-Garbarino-Brecheen-to-Noem-DHS-re-Volt-and-Salt-Typhoon.pdf.

25 Dustin Volz, "In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks," *Wall Street Journal*, April 10, 2025, https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb.

26 Littleton Electric Light and Water Departments, "LELWD Publicizes Case Study on Foreign Hackers Targeting U.S. Utilities," March 14, 2025, https://www.lelwd.com/cybersecurity-case-study/; Jonathan Greig, "Volt Typhoon Hackers Were in Massachusetts Utility Systems for 10 Months," *The Record*, September 9, 2025, https://therecord.media/volt-typhoon-hackers-utility-months; Eduard Kovacs, "China's Volt Typhoon Hackers Dwelled in U.S. Electric Grid for 300 Days," *SecurityWeek*, March 12, 2025, https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/.

27 Miguel Yañez-Barnuevo, "Data Centers and Water Consumption," Environmental and Energy Study Institute, June 20, 2025, https://www.eesi.org/articles/view/data-centers-and-water-consumption; Yoon Young Chung, Federico Darakdjian, Tom Leahy, "When AI Meets Water Scarcity: Data Centers in a Thirsty World," December 9, 2025, https://www.msci.com/research-and-insights/blog-post/

when-ai-meets-water-scarcity-data-centers-in-a-thirsty-world.

28 McKael Kirwin, "Texas Data Centers Thirst for Water, Challenging State Infrastructure," August 6, 2025, https://texasscorecard.com/state/texas-data-centers-thirst-for-water-challenging-state-infrastructure/.

29 "Annual Data Center Outages Analysis 2026," Uptime Institute, accessed June 21, 2026, https://uptimeinstitute.com/resources/research-and-reports/annual-outages-analysis-2026.

30 Robert Walton, "NERC Is 'Actively Monitoring the Grid' Following Iran-Linked Cyber Threat," *Utility Dive*, April 8, 2026, https://www.utilitydive.com/news/nerc-cisa-iran-war-cyber-hacking/816914/.

31 Ibid.

32 U.S. Senate Committee on Environment and Public Works, "Identifying and Addressing Cybersecurity Challenges to Protect America's Water Infrastructure," February 4, 2026, https://www.epw.senate.gov/public/_cache/files/5/3/53137704-c977-4e5e-b03c-22881319cc9d/1BB9703FC4943AB36FF8B981F387DD5BB37092843C78130ABF3908814DC1EBAF.spw-02042026-identifying-and-addressing-cybersecurity-challenges-to-protect-america-s-water-infrastructure.pdf.

33 Jason Healey, Former White House Cyber Directorate, interviewed by the authors, April 2, 2026; Nuno Marques, Deputy Mayor of Notodden, Norway, and International Law Scholar, interviewed by Jennifer Bassett, March 27, 2026.

34 Cybersecurity and Infrastructure Security Agency, "Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization," Joint Cybersecurity Advisory AA24-326A, November 21, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a.

35 North American Electric Reliability Corporation, CIP Standards Roadmap (Atlanta: NERC, January 12, 2026), 35, https://www.nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf.

36 Xin Chen et al., "Electricity Demand and Grid Impacts of AI Data Centers: Challenges and Prospects," Texas A&M University, November 26, 2025, https://arxiv.org/pdf/2509.07218.

37 Federal Energy Regulatory Commission, "Order Regarding Intent to Act, Interconnection of Large Loads to the Interstate Transmission System, Docket No. RM26-4-000," FERC, April 16, 2026, https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20260416-3003&optimized=false&sid=a0742aa8-47f0-45e9-bec0-e42b1141e08c.

38 General Services Administration, "About FedRAMP," accessed April 8, 2026, https://www.fedramp.gov/about/.

39 Federal Data Center Enhancement Act of 2023, https://www.congress.gov/bill/118th-congress/house-bill/5218/text#HCA7EA626AB404CFDB0155A96D5DD11B6.

40 National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 1543, 139 Stat. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/1071.

41 White House, National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), April 30, 2024, https://www.presidency.ucsb.edu/documents/national-security-memorandum-critical-infrastructure-security-and-resilience.

42 Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed April 8, 2026, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

43 White House, "America's AI Action Plan," July 23, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

44 Jeremy Hsu, "Drone strikes on data centers spook Big Tech, halting Middle East projects," ars technica, April 29, 2026, https://arstechnica.com/ai/2026/04/data-center-developer-pauses-middle-east-projects-after-war-damage/.

45 Klaudia Klonowska and Michael Schmitt, "Iranian Attacks on the Amazon Data Centers: A Legal Analysis," Just Security, March 12, 2026, https://www.justsecurity.org/133685/iranian-attacks-amazon-data-centers-legal-analysis/.

46 OpenAI, "Introducing OpenAI for Countries," May 7, 2025, https://openai.com/global-affairs/openai-for-countries/.

47 Alibaba Cloud, "Alibaba Cloud Launches Second Data Center in Dubai to Accelerate AI-Powered Digitalization in the Middle

East," October 14, 2025, https://www.alibabacloud.com/blog/alibaba-cloud-launches-second-data-center-in-dubai-to-accelerate-ai-powered-digitalization-in-the-middle-east_602595.

48 National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 1543, 139 Stat. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/1071.

49 Katherine Blunt, "America's Data-Center Build-Out Is Falling Way Behind Schedule," *Wall Street Journal*, June 3, 2026, https://www.wsj.com/tech/ai/americas-data-center-build-out-is-falling-way-behind-schedule-e408a9a8?mod=hp_lead_pos1; Olivia Wang, "Data Center Outlook," Sightline Climate, February 24, 2026, https://www.sightlineclimate.com/research/data-center-outlook.

50 Ramaswamy Chandramouli and Doron Pinhas, "NIST Special Publication 800-209: Security Guidelines for Storage Infrastructure, National Institute of Standards and Technology, U.S. Department of Commerce, October 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf.

51 Ibid.

52 https://www.brookings.edu/articles/global-energy-demands-within-the-ai-regulatory-landscape/

53 "NERC Issues Level 2 Alert for "Large Loads"", Duncan Weinberg Genzer & Pembroke, 11 September, 2025, https://dwgp.com/firm-announcements/nerc-issues-level-2-alert-for-large-loads.

54 Rachel Mural, Dipesh Pherwani and Chaitanya Gupta, "Data Centers and Large-Scale Electric Growth: The Virginia and Texas Experiences," Harvard Kennedy School, April 20, 2026, https://www.belfercenter.org/research-analysis/data-centers-texas-virginia-comparison.

55 Travis Fisher and Glen Lyons, "Texas Is Building the Future of Electricity," *Cato Institute*, April 10, 2026, https://www.cato.org/blog/texas-building-future-electricity; Paul Colber, "Texas forecast to be top market for data centers in two years, increasing grid demand," The Texas Turbine, January 20, 2026, https://www.texastribune.org/2026/01/20/texas-top-data-center-market-power-grid/.

56 Spencer Kimball, "Google to Invest $25 Billion in Data Centers and AI Infrastructure Across Largest U.S. Electric Grid," *CNBC*, July 15, 2025, https://www.cnbc.com/2025/07/15/google-to-invest-25-billion-in-data-centers-ai-infrastructure-in-pjm.htm.

57 Ethan Howland, "PJM Board Calls for Backstop Auction in Data Center Interconnection Plan," *Utility Dive*, January 20, 2026, https://www.utilitydive.com/news/pjm-board-backstop-auction-data-center-interconnection/809967/.

58 Zachary Skidmore, "Dominion Reports Marginal Increase in Data Center Pipeline," *Data Center Dynamics*, February 24, 2026, https://www.datacenterdynamics.com/en/news/dominion-reports-marginal-increase-in-data-center-pipeline/.

59 General Services Administration, "About FedRAMP," accessed April 8, 2026, https://www.fedramp.gov/about/.

60 https://www.jll.com/en-us/insights/market-dynamics/north-america-data-centers

61 Federal Energy Regulatory Commission, "Explainer on the Interconnection Final Rule," FERC, last updated January 23, 2025, https://www.ferc.gov/explainer-interconnection-final-rule.

62 Federal Energy Regulatory Commission, "FERC Strengthens Order No. 1920 with Expanded State Provisions," FERC, November 21, 2024, https://www.ferc.gov/news-events/news/ferc-strengthens-order-no-1920-expanded-state-provisions.

63 Federal Energy Regulatory Commission, "FERC's Grid Work Continues Amid Order No. 2023 Compliance," FERC, September 25, 2024, https://www.ferc.gov/news-events/news/fercs-grid-work-continues-amid-order-no-2023-compliance

64 Cybersecurity and Infrastructure Security Agency, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities," Joint Cybersecurity Advisory AA23-335A, December 1, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

65 Securing Reliable Power for Advanced Technologies Act, H.R. 5927, 119th Cong. (2025).

.

For additional details on methodology and findings, contact ASP at press@americansecurityproject.org.